

# **Procedures supporting the Use of Communication and Information Technology Devices Policy**

## **Access to office mobile telephones**

Mobile telephones are allocated to statutory officers and certain members of staff, as determined from time-to-time by the Ombudsman, who require the use of a mobile telephone to effectively perform their functions.

Mobile telephones are also allocated to each team for use by team members when they are required to work away from the office and need the use of a mobile telephone to effectively perform their functions.

When you take possession of a mobile telephone allocated to your team you must record the following details in the mobile telephone register (to be maintained by the executive assistant or a team assistant):

- The date you took possession of the telephone
- your name
- the mobile telephone number
- your signature.

When you return the telephone, you must place it back in secure storage and record the following details in the register:

- the date you returned the telephone
- your signature.

## **Access to office portable computers**

The office's portable computers are kept in the IT section in a secure cupboard accessible only by the help desk officer.

If you wish to use a portable computer, contact the help desk officer to find out if there is a computer available. Before you take possession of a portable computer, you must record the following details in the portable computer register (to be maintained by the help desk officer):

- the date you took possession of the computer
- your name
- the identifying number of the computer
- your signature.

You must return the portable computer to the help desk officer. **DO NOT** leave it unattended in their office. You must also record the following details in the register:

- the date you returned the computer
- your signature.

## **Monitoring and release of blocked emails**

### **General**

Mail filtering is necessary to protect the office computer network from constant threats in the form of emails. These include viruses which allow people to access our confidential files, viruses which corrupt our data, or spam which can slow down our entire network.

To counteract the thousands of emails sent to staff which may contain viruses or which may be spam, the office uses software to automatically filter all inbound emails. This means an email may be automatically diverted into a safe file accessible only by IT staff before it reaches an inbox.

The rules for determining which emails should be filtered are constantly changing, in order to deal with spam or virus threats which become more sophisticated over time. Therefore, on occasion, more emails may be diverted than usual. IT staff will alert the office when a major new threat has been identified.

Procedures for IT staff to manually release mail is set out in the IT SOPs manual.

### **Mail Marshal**

*Mail Marshal* will be manually checked by IT staff 3 times daily for legitimate blocked mail, as per the Use of Communication and Information Technology Devices Policy. All mail deemed to be unnecessarily blocked will be released.

All *Mail Marshal* rule sets are documented in the IT SOPs manual. Changes to rule sets require a change approval form.

Users are notified of blocked mail except for messages that are deemed to be spam or to contain a virus. This is consistent with policy and guidelines issued by the NSW Premiers Department.

In practice, users should notify IT helpdesk of a message that they need released, however IT staff may release messages that users have not yet requested for release. Any request is logged in the Help Desk database.

### **Guide for staff about what types of emails will be blocked**

All incoming and out going mail is scanned electronically.

Any message that may contain a potential threat to the network, or does not meet policy, is quarantined by the system.

Staff will be notified of quarantined mail, except if the message contains a virus, or is spam.

IT staff will manually review the content of the quarantined messages, and release any messages that do not pose a threat, except if the message contains a virus or is spam.

If a staff member requires an e-mail release urgently, contact IT staff to have it released.

If a staff member is missing an e-mail, contact the IT Help desk for further assistance.

### **Threats to the network**

The following are considered threats to the network, and are blocked. In general these messages are not released:

- virus, worms or trojans - these are quarantined, and not released, and the user is not notified
- spam - any message deemed to be spam is blocked, and the user is not notified
- malformed messages - messages that do not conform to e-mail standards, or are fragmented, are blocked, and the user is not notified.

If a staff member is missing an email, request IT staff to check that it has not been automatically blocked.

### **Potential threats to the network**

The following messages are blocked, and manually released, after review by IT staff:

- compressed files such as, ZIP, ARJ, RAR
- files with Double extensions, eg: document.doc.jpg, or document.1.doc
- files with attached shortcuts
- files with an unknown file type
- files over 8mb in size
- junk mail, such as chain letters, the Jamie Oliver cookbook, personality test etc. In general, junk mail will not be released.